UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/537,705	06/03/2005	Tim Neil	93422-47	5122

22463 7590 01/08/2009

SMART AND BIGGAR
438 UNIVERSITY AVENUE
SUITE 1500 BOX 111
TORONTO, ON M5G2K8
CANADA

EXAMINER	
TURNER, ASHLEY D	
ART UNIT	PAPER NUMBER
2454	

MAIL DATE	DELIVERY MODE
01/08/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/537,705	NEIL ET AL.	
	Examiner	Art Unit	
	ASHLEY D. TURNER	2454	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/3/2005, 9/30/2005,6/16/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-24 are rejected under 35 U.S.C. 102 (b) as being anticipated by Ransom et al hereinafter Ransom (US 2004/0107025 A1).

Regarding claim 1

Referring to claim 1 Ransom discloses a method of determining operational status of a wireless communication device capable of executing server-side applications, the method comprising: sending a message to said wireless communication device (Parargraph [0050] The switching layer interfaces the routing layer to the interface layer. The switching layer and interface layer are typically integrated. The interface layer comprises the actual hardware interface to the network. The interface layer may include an Ethernet interface, a modem, such as wired modem using the serial line interface protocol ("SLIP") or point to point protocol ("PPP"), wired modem which may be an analog or digital modem such as a integrated services digital network ("ISDN") modem or digital subscriber line ("DSL") modem, or a cellular modem. Further, other wireless interfaces, such as Bluetooth, may also be used. In addition, AC power line data network interface may also be used. Cellular modems further provide the functionality to determine the geographic location of the IED using cellular RF triangulation. Such location information can be

transmitted along with other power management data as one factor used in authenticating the transmitted data. In the preferred embodiments, the interface layer provided allows for redundant communication capabilities. The interface layer couples the IED with a local area network, such as provided at the customer or utility site. Alternatively, the interface layer can couple the IED with a point of presence provided by a local network provider such as an internet service provider ("ISP").) capable of executing server-side applications i.e. power management application requesting operational status i.e. minimize or maximize of the device; and receiving a response message i.e. computed values such as revenue, cost, consumption or usage by use of handling and manipulating power systems and load routing. IED inventory, maintenance and fraud detection component 261, 262, 263 receive or request communications from the IED's 102-109 allowing the power management application to inventory the installed base of IED's 102-109, from said wireless communication device indicative of the operational status of the device. (Paragraph [0065] In the preferred embodiment, the data collection component 250 enables an IED to collect and collate data from either a single or multiple sources via the network 110. The data collected by the component is stored and can be retrieved by other components of the power management application components 290, or other components implemented on other IED's 102-109 located on the network 110. In the preferred embodiment the Automated Meter Reading component 253 is utilized to allow either the consumers 132, 133 or providers 130, 131 to generate power management reports from the IED data. In the preferred embodiment the electrical power generation management component 260 analyzes data received from IED's 102-109 to either minimize or maximize measured or computed values such as revenue, cost, consumption or usage by use of handling and manipulating power systems and load routing. IED

inventory, maintenance and fraud detection component 261, 262, 263 receive or request communications from the IED's 102-109 allowing the power management application to inventory the installed base of IED's 102-109, including establishing or confirming their geographic installation location, or check the maintenance history of all connected IED's 102-109 These power management applications aid in confirming outage locations or authenticating communications to or from an IED 102-109 to prevent fraud and minimize errors. In one embodiment, the IED inventory component 261 utilizes cellular triangulation technologies, or caller ID based geographic locator technologies to determine and verify IED inventories. In the preferred embodiment the fraud detection component 263 further detects device tampering. In the preferred embodiment the power quality monitoring component 264 monitors and processes electric parameters, such as current, voltage and energy which include volts, amps, Watts, phase relationships between waveforms, kWh, kvAr, power factor, and frequency, etc. The power quality monitoring component 264 reports alarms, alerts, warnings and general power quality status, based on the monitored parameters, directly to the appropriate user, such as customers 132, 133 or utilities 130, 131.)

Regarding claim 13

Claim 13 is similarly rejected using the same reasoning / citations provided above for claim 1 since they recite the same limitations and are distinguished only by statutory category.

Regarding claim 2

Referring to claim 2 Ransom discloses all the limitations of claim 2 which is described above. Ransom also discloses wherein said operational status of the wireless communication device comprises an indication of N most recent errors occurring at said wireless communication device, where N is an integer. (Paragraph [0060] Furthermore, the application 111 includes an authentication and encryption component which encrypts commands transmitted across the network 110, and decrypts power management data received over the network 110. Authentication is also performed for commands or data sent or received over the network 110. Authentication is the process of determining and verifying whether the IED 102-109 transmitting data or receiving commands is the IED 102-109 it declares itself to be and in the preferred embodiment authentication includes parameters such as time/date stamps, digital certificates, physical locating algorithms such as cellular triangulation, serial or tracking ID's, which could include geographic location such as longitude and latitude. Authentication prevents fraudulent substitution of IED 102-109 devices or spoofing of IED 102-109 data generation in an attempt to defraud. Authentication also minimizes data collection and power distribution system 101 control errors by verifying that data is being generated and commands are being received by the appropriate devices. In the preferred embodiment encryption is done utilizing Pretty Good Privacy (PGP). PGP uses a variation of public key system, where each user has a publicly known encryption key and a private key known only to that user. The public key system and

infrastructure enables users of unsecured networks, such as the internet, to securely and privately exchange data through the use of public and private cryptographic key pairs.)

Regarding claim 14

Claim 14 is similarly rejected using the same reasoning / citations provided above for claim 2 since they recite the same limitations and are distinguished only by statutory category.

Regarding claim 3

Referring to claim 3 Ransom discloses all the limitations of claim 3 which is described above. Ransom also discloses wherein said operational status of the wireless communication device comprises an indication of N messages most frequently received at said device, where N is an integer. (Paragraph [0065] In the preferred embodiment, the data collection component 250 enables an IED to collect and collate data from either a single or multiple sources via the network 110. The data collected by the component is stored and can be retrieved by other components of the power management application components 290, or other components implemented on other IED's 102-109 located on the network 110. In the preferred embodiment the Automated Meter Reading component 253 is utilized to allow either the consumers 132, 133 or providers 130, 131 to generate power management reports from the IED data. In the preferred embodiment the electrical power generation management component 260 analyzes data received

from IED's 102-109 to either minimize or maximize measured or computed values such as revenue, cost, consumption or usage by use of handling and manipulating power systems and load routing. IED inventory, maintenance and fraud detection component 261, 262, 263 receive or request communications from the IED's 102-109 allowing the power management application to inventory the installed base of IED's 102-109, including establishing or confirming their geographic installation location, or check the maintenance history of all connected IED's 102-109 These power management applications aid in confirming outage locations or authenticating communications to or from an IED 102-109 to prevent fraud and minimize errors. In one embodiment, the IED inventory component 261 utilizes cellular triangulation technologies, or caller ID based geographic locator technologies to determine and verify IED inventories. In the preferred embodiment the fraud detection component 263 further detects device tampering. In the preferred embodiment the power quality monitoring component 264 monitors and processes electric parameters, such as current, voltage and energy which include volts, amps, Watts, phase relationships between waveforms, kWh, kvAr, power factor, and frequency, etc. The power quality monitoring component 264 reports alarms, alerts, warnings and general power quality status, based on the monitored parameters, directly to the appropriate user, such as customers 132, 133 or utilities 130, 131.)

Regarding claim15

Claim 15 is similarly rejected using the same reasoning / citations provided above for claim 3 since they recite the same limitations and are distinguished only by statutory category.

Regarding claim 4

Referring to claim 4 Ransom discloses all the limitations of claim 4 which is described above. Ransom also discloses wherein said operational status of the wireless communication device comprises an indication of a user interface screen currently displayed at said device. (Paragraph [0097] Referring to FIG. 11, there is shown an exemplary screen display of a Microsoft Excel worksheet which is coupled with the IED 1002 as described above. In this example, the IED 1002 is a model 8500 meter, manufactured by Power Measurement Limited, in Victoria, British Columbia, Canada. The IED 1002 is coupled via a TCP/IP based network with a personal computer having at least 64 MB memory and 6 GB hard disk with a Pentium.TM. III or equivalent processor or better, executing the Microsoft Windows 98.TM. operating system and Microsoft Excel 2000. The computer further includes Microsoft Internet Explorer.TM. 5.0 which includes an XML parser that receives and parses the XML data fro the meter and delivers it to the Excel worksheet. The worksheet displays real time data received directly from the IED 1002 in an XML format. As the IED 1002 detects and measures fluctuations in the delivered electrical power, it transmits updated information, via XML, to the worksheet which, in turn, updates the displayed data in real time. Note that all of the features of the Microsoft Excel program are available to manipulate and analyze the received real time data, including the ability to specify mathematical formulas and complex equations which act on the data. Further, display templates

and charting/graphing functions can be implemented to provide meaningful visual analysis of the data as it is received. Further, the real time data can be logged for historical analysis. In one embodiment, the activation of a new IED 1002 on the network is detected by the worksheet which cause automatic generation of a new worksheet to receive and display data from the new device.)

Regarding claim 16

Claim 16 is similarly rejected using the same reasoning / citations provided above for claim 4 since they recite the same limitations and are distinguished only by statutory category.

Regarding claim 5

Referring to claim 5 Ransom discloses all the limitations of claim 5 which is described above. Ransom also discloses wherein said operational status of the wireless communication device comprises a network identifier identifying a wireless network over which said device is communicating. (Paragraph [0065] In the preferred embodiment, the data collection component 250 enables an IED to collect and collate data from either a single or multiple sources via the network 110. The data collected by the component is stored and can be retrieved by other

components of the power management application components 290, or other components implemented on other IED's 102-109 located on the network 110. In the preferred embodiment the Automated Meter Reading component 253 is utilized to allow either the consumers 132, 133 or providers 130, 131 to generate power management reports from the IED data. In the preferred embodiment the electrical power generation management component 260 analyzes data received from IED's 102-109 to either minimize or maximize measured or computed values such as revenue, cost, consumption or usage by use of handling and manipulating power systems and load routing. IED inventory, maintenance and fraud detection component 261, 262, 263 receive or request communications from the IED's 102-109 allowing the power management application to inventory the installed base of IED's 102-109, including establishing or confirming their geographic installation location, or check the maintenance history of all connected IED's 102-109 These power management applications aid in confirming outage locations or authenticating communications to or from an IED 102-109 to prevent fraud and minimize errors. In one embodiment, the IED inventory component 261 utilizes cellular triangulation technologies, or caller ID based geographic locator technologies to determine and verify IED inventories. In the preferred embodiment the fraud detection component 263 further detects device tampering. In the preferred embodiment the power quality monitoring component 264 monitors and processes electric parameters, such as current, voltage and energy which include volts, amps, Watts, phase relationships between waveforms, kWh, kvAr, power factor, and frequency, etc.)

Regarding claim 17

Claim 17 is similarly rejected using the same reasoning / citations provided above for claim 5 since they recite the same limitations and are distinguished only by statutory category.

Regarding claim 6

Referring to claim 6 Ransom discloses all the limitations of claim 6 which is described above. Ransom also discloses wherein said operational status of the wireless communication device comprises an indication of a make and model of said wireless communication device. (Paragraph [0065] In the preferred embodiment, the data collection component 250 enables an IED to collect and collate data from either a single or multiple sources via the network 110. The data collected by the component is stored and can be retrieved by other components of the power management application components 290, or other components implemented on other IED's 102-109 located on the network 110. In the preferred embodiment the Automated Meter Reading component 253 is utilized to allow either the consumers 132, 133 or providers 130, 131 to generate power management reports from the IED data. In the preferred embodiment the electrical power generation management component 260 analyzes data received from IED's 102-109 to either minimize or maximize measured or computed values such as revenue, cost, consumption or usage by use of handling and manipulating power systems and load routing. IED inventory, maintenance and fraud detection component 261, 262, 263 receive or request communications from the IED's 102-109 allowing the power management application to inventory the installed base of IED's 102-109, including establishing or confirming their geographic installation

location, or check the maintenance history of all connected IED's 102-109 These power management applications aid in confirming outage locations or authenticating communications to or from an IED 102-109 to prevent fraud and minimize errors. In one embodiment, the IED inventory component 261 utilizes cellular triangulation technologies, or caller ID based geographic locator technologies to determine and verify IED inventories. In the preferred embodiment the fraud detection component 263 further detects device tampering. In the preferred embodiment the power quality monitoring component 264 monitors and processes electric parameters, such as current, voltage and energy which include volts, amps, Watts, phase relationships between waveforms, kWh, kvAr, power factor, and frequency, etc.)

Regarding claim 18

Claim 18 is similarly rejected using the same reasoning / citations provided above for claim 6 since they recite the same limitations and are distinguished only by statutory category.

Regarding claim 7

Referring to claim 7 Ransom discloses all the limitations of claim 7 which is described above. Ransom also discloses wherein said operational status of the wireless communication device comprises an indication of power remaining at said wireless communication device. (Paragraph [0005] the present invention is defined by the following claims and nothing in this section should

be taken as a limitation on those claims. By way of introduction, the preferred embodiments described below relate to an energy management device for managing the flow of energy in an energy distribution system, the energy management device for use in an energy management architecture for managing the energy distribution system, the energy management architecture comprising a network. The energy management device includes: a network interface operative to couple the energy management device with the network; an energy distribution system interface operative to couple the energy management device with the energy distribution system, the energy management device further operative to measure at least one energy management quantity via the energy distribution system interface; a processor coupled with the network interface and the energy distribution system interface and operative to process the at least one energy management quantity to manage the flow of electrical energy; and wherein the network interface is further operative to incrementally receive one of a power management command and power management data encoded as an XML document from the network, the XML document being received as a plurality of segments, wherein the network interface is capable of processing at least one received of the plurality of segments and extracting the one of the power management command and power management data therefrom prior to receiving all of the plurality of segments.)

Regarding claim 19

Claim 19 is similarly rejected using the same reasoning / citations provided above for claim 7 since they recite the same limitations and are distinguished only by statutory category.

Regarding claim 8

Referring to claim 8 Ransom discloses all the limitations of claim 8 which is described above. Ransom also discloses wherein said operational status of the wireless communication device comprises an indication of available memory at said wireless communication device. (Paragraph [0097] Referring to FIG. 11, there is shown an exemplary screen display of a Microsoft Excel worksheet which is coupled with the IED 1002 as described above. In this example, the IED 1002 is a model 8500 meter, manufactured by Power Measurement Limited, in Victoria, British Columbia, Canada. The IED 1002 is coupled via a TCP/IP based network with a personal computer having at least 64 MB memory and 6 GB hard disk with a Pentium.TM. III or equivalent processor or better, executing the Microsoft Windows 98.TM. operating system and Microsoft Excel 2000. The computer further includes Microsoft Internet Explorer.TM. 5.0 which includes an XML parser that receives and parses the XML data fro the meter and delivers it to the Excel worksheet. The worksheet displays real time data received directly from the IED 1002 in an XML format. As the IED 1002 detects and measures fluctuations in the delivered electrical power, it transmits updated information, via XML, to the worksheet which, in turn, updates the displayed data in real time. Note that all of the features of the Microsoft Excel program are available to manipulate and analyze the received real time data, including the ability to specify mathematical formulas and complex equations which act on the data. Further, display templates and charting/graphing functions can be implemented to provide meaningful visual analysis of the

data as it is received. Further, the real time data can be logged for historical analysis. In one embodiment, the activation of a new IED 1002 on the network is detected by the worksheet which cause automatic generation of a new worksheet to receive and display data from the new device.)

Regarding claim 20

Claim 20 is similarly rejected using the same reasoning / citations provided above for claim 8 since they recite the same limitations and are distinguished only by statutory category.

Regarding claim 9

Referring to claim 9 Ransom discloses A method of providing the operational status of a wireless communication device capable of executing server-side applications, the method comprising: receiving a message at said wireless communication device capable of executing server-side applications requesting operational status of the device, said receiving resulting in a received message; composing a response message from said wireless communication device indicative of the operational status of the device; and sending said response message from said wireless communication device to an originator of said received message. (Paragraph [0065] In the preferred embodiment, the data collection component 250 enables an IED to collect and collate

data from either a single or multiple sources via the network 110. The data collected by the component is stored and can be retrieved by other components of the power management application components 290, or other components implemented on other IED's 102-109 located on the network 110. In the preferred embodiment the Automated Meter Reading component 253 is utilized to allow either the consumers 132, 133 or providers 130, 131 to generate power management reports from the IED data. In the preferred embodiment the electrical power generation management component 260 analyzes data received from IED's 102-109 to either minimize or maximize measured or computed values such as revenue, cost, consumption or usage by use of handling and manipulating power systems and load routing. IED inventory, maintenance and fraud detection component 261, 262, 263 receive or request communications from the IED's 102-109 allowing the power management application to inventory the installed base of IED's 102-109, including establishing or confirming their geographic installation location, or check the maintenance history of all connected IED's 102-109 These power management applications aid in confirming outage locations or authenticating communications to or from an IED 102-109 to prevent fraud and minimize errors. In one embodiment, the IED inventory component 261 utilizes cellular triangulation technologies, or caller ID based geographic locator technologies to determine and verify IED inventories. In the preferred embodiment the fraud detection component 263 further detects device tampering. In the preferred embodiment the power quality monitoring component 264 monitors and processes electric parameters, such as current, voltage and energy which include volts, amps, Watts, phase relationships between waveforms, kWh, kvAr, power factor, and frequency, etc. The power quality monitoring component 264 reports alarms, alerts, warnings and general power quality

status, based on the monitored parameters, directly to the appropriate user, such as customers 132, 133 or utilities 130, 131.)

Regarding claim 21

Claim 21 is similarly rejected using the same reasoning / citations provided above for claim 9 since they recite the same limitations and are distinguished only by statutory category.

Regarding claim 10

Referring to claim 10 Ransom discloses all the limitations of claim 10 which is described above. Ransom also discloses wherein said response message is an eXtensible Markup Language (XML) message. (Paragraph [0006] The preferred embodiments further relate to a method, in an energy management device, of transmitting a communication from the energy management device over a network coupled with the energy management device. In one embodiment, the method includes: generating a set of data to be communicated over the network as an XML document; transforming each of the data into an XML format as it is generated; and communicating each of the XML formatted data over the network as it is transformed; releasing at least one resource utilized by the XML formatted data from the energy management device as

it is communicated; and repeating the transforming and the communicating until the entire the set of data has been communicated.

Regarding claim 22

Claim is similarly rejected using the same reasoning / citations provided above for claim 10 since they recite the same limitations and are distinguished only by statutory category.

Regarding claim 11

Referring to claim 11 Ransom discloses all the limitations of claim 11 which is described above. Ransom also discloses wherein said composing comprises verifying that a textual operational status description forming part of said response message omits illegal XML characters. (Paragraph [0128] In one embodiment of the incremental XML processing system described herein, the capability to handle errors is provided. Errors may occur if one or more processable segments of the XML document are too large to fit in the IED's available memory, are corrupted or otherwise comprised or the segment contains unrecognized or improper XML code, data or commands. When incrementally processing received XML, it is possible that many processable segments will be successfully processed prior to an error occurring. For a given XML document, it may be okay that only a portion of the overall file was successfully processed. In this case, the IED can attempt to re-request the unsuccessfully processed segment(s) or continue operations

without those segment(s). Typically, however, if the entire XML document cannot be processed then none of the XML document should be processed. This may be the case for an XML document which contains a set of configuration commands and data. In such a case, partial configuration may result in an inoperable IED. Therefore, in one embodiment, a mechanism is provided which permits the IED to undo any completed processing the XML document when an error occurs. In one embodiment, the IED is capable of saving the complete operational state of the device prior to commencing processing of the XML document, or a processable segment thereof, and restoring that state should an error occur. In embodiments that are incapable of reversing the partial execution of the XML document, the XML document generator generates the XML code such that errors in processing some of the code does not affect the successfully processed code.

Regarding claim 15 and 23

Claim 23 is similarly rejected using the same reasoning / citations provided above for claim 11 since they recite the same limitations and are distinguished only by statutory category.

Regarding claim 12

Referring to claim 12 Ransom discloses all the limitations of claim 12 which is described above. Ransom also discloses wherein said verifying comprises passing said textual operational status

description through an XML formatter for removal of any illegal XML characters. (Paragraph [0128] In one embodiment of the incremental XML processing system described herein, the capability to handle errors is provided. Errors may occur if one or more processable segments of the XML document are too large to fit in the IED's available memory, are corrupted or otherwise comprised or the segment contains unrecognized or improper XML code, data or commands. When incrementally processing received XML, it is possible that many processable segments will be successfully processed prior to an error occurring. For a given XML document, it may be okay that only a portion of the overall file was successfully processed. In this case, the IED can attempt to re-request the unsuccessfully processed segment(s) or continue operations without those segment(s). Typically, however, if the entire XML document cannot be processed then none of the XML document should be processed. This may be the case for an XML document which contains a set of configuration commands and data. In such a case, partial configuration may result in an inoperable IED. Therefore, in one embodiment, a mechanism is provided which permits the IED to undo any completed processing the XML document when an error occurs. In one embodiment, the IED is capable of saving the complete operational state of the device prior to commencing processing of the XML document, or a processable segment thereof, and restoring that state should an error occur. In embodiments that are incapable of reversing the partial execution of the XML document, the XML document generator generates the XML code such that errors in processing some of the code does not affect the successfully processed code.

Regarding claim 24

Claim 24 is similarly rejected using the same reasoning / citations provided above for claim 12 since they recite the same limitations and are distinguished only by statutory category.

Response to Arguments

Applicant's arguments filed on 9/24/08 have been fully considered but they are not persuasive.

Summary and Response to Arguments

A. Applicant argues the rejection under 35 U.S.C. 102(b) under Ransom for claims 1,9,13, 21 as Ransom does not disclose the claimed limitations, as Ransom does not discloses a wireless communication device; capable of executing server-side applications.

As to point A, applicant's arguments are not persuasive, as in the context of a wireless communication device; capable of executing server-side applications. The examiner respectfully disagrees with applicant assertions. Reference A discloses that the IED is using multiple protocol such as Bluetooth and cellar Radio Frequency is utilized by IED. The power managment application is the server-side applications that are communicating to the IEDS. (Parargraph [0050] The switching layer interfaces the routing layer to the interface layer. The switching layer and interface layer are typically integrated. The interface layer comprises the actual hardware interface to the network. The interface layer may include an Ethernet interface, a modem, such as wired modem using the serial line interface protocol ("SLIP") or point to point protocol ("PPP"),

wired modem which may be an analog or digital modem such as a integrated services digital network ("ISDN") modem or digital subscriber line ("DSL") modem, or a cellular modem. Further, other wireless interfaces, such as Bluetooth, may also be used. In addition, AC power line data network interface may also be used. Cellular modems further provide the functionality to determine the geographic location of the IED using cellular RF triangulation.) Examiner gave the broadest interpretation to the claim language. Applicants arguments to the claims failed to overcome the teaching of Ransom. (Paragraph [0065] In the preferred embodiment, the data collection component 250 enables an IED to collect and collate data from either a single or multiple sources via the network 110. The data collected by the component is stored and can be retrieved by other components of the power management application components 290, or other components implemented on other IED's 102-109 located on the network 110. In the preferred embodiment the Automated Meter Reading component 253 is utilized to allow either the consumers 132, 133 or providers 130, 131 to generate power management reports from the IED data. In the preferred embodiment the electrical power generation management component 260 analyzes data received from IED's 102-109 to either minimize or maximize measured or computed values such as revenue, cost, consumption or usage by use of handling and manipulating power systems and load routing. IED inventory, maintenance and fraud detection component 261, 262, 263 receive or request communications from the IED's 102-109 allowing the power management application to inventory the installed base of IED's 102-109, including establishing or confirming their geographic installation location, or check the maintenance history of all connected IED's 102-109 These power management applications aid in confirming outage locations or authenticating communications to or from an IED 102-109 to prevent fraud

and minimize errors. In one embodiment, the IED inventory component 261 utilizes cellular triangulation technologies, or caller ID based geographic locator technologies to determine and verify IED inventories. In the preferred embodiment the fraud detection component 263 further detects device tampering. In the preferred embodiment the power quality monitoring component 264 monitors and processes electric parameters, such as current, voltage and energy which include volts, amps, Watts, phase relationships between waveforms, kWh, kvAr, power factor, and frequency, etc. The power quality monitoring component 264 reports alarms, alerts, warnings and general power quality status, based on the monitored parameters, directly to the appropriate user, such as customers 132, 133 or utilities 130, 131). Examiner gave the broadest interpretation to the claim language. Applicants arguments to the claim failed to overcome the teaching of Ransom.

B. Applicant argues the rejection under 35 U.S.C. 102(b) under Ransom for claims 2 and 14 as Ransom does not disclose the claimed limitations, as Ransom does not disclose wherein said operational status of the wireless communication device comprises an indication of N most recent errors occurring at said wireless communication device where N is an integer.

As to point B, applicant's arguments are not persuasive, as in the context of wherein said operational status of the wireless communication device comprises an indication of N most recent errors occurring at said wireless communication device where N is an integer. The examiner respectfully disagrees with applicant assertions. Reference A discloses the number of

data being sent by the IEDS to the electric power distribution system "many of the messages" which are computed values such as cost, revenue, consumption. The operational statuses are the minimized or maximized measured. (Paragraph [0065] In the preferred embodiment, the data collection component 250 enables an IED to collect and collate data from either a single or multiple sources via the network 110. The data collected by the component is stored and can be retrieved by other components of the power management application components 290, or other components implemented on other IED's 102-109 located on the network 110. In the preferred embodiment the Automated Meter Reading component 253 is utilized to allow either the consumers 132, 133 or providers 130, 131 to generate power management reports from the IED data. In the preferred embodiment the electrical power generation management component 260 analyzes data received from IED's 102-109 to either minimize or maximize measured or computed values such as revenue, cost, consumption or usage by use of handling and manipulating power systems and load routing. IED inventory, maintenance and fraud detection component 261, 262, 263 receive or request communications from the IED's 102-109 allowing the power management application to inventory the installed base of IED's 102-109, including establishing or confirming their geographic installation location, or check the maintenance history of all connected IED's 102-109 These power management applications aid in confirming outage locations or authenticating communications to or from an IED 102-109 to prevent fraud and minimize errors. In one embodiment, the IED inventory component 261 utilizes cellular triangulation technologies, or caller ID based geographic locator technologies to determine and verify IED inventories. In the preferred embodiment the fraud detection component 263 further detects device tampering. In the preferred embodiment the power quality monitoring component

264 monitors and processes electric parameters, such as current, voltage and energy which include volts, amps, Watts, phase relationships between waveforms, kWh, kvAr, power factor, and frequency, etc. The power quality monitoring component 264 reports alarms, alerts, warnings and general power quality status, based on the monitored parameters, directly to the appropriate user, such as customers 132, 133 or utilities 130, 131.) Examiner gave the broadest interpretation to the claim language. Applicants arguments to the claim failed to overcome the teaching of Ransom.

C. Applicant argues the rejection under 35 U.S.C. 102(b) under Ransom for claims 3 and 15 as Ransom does not disclose the claimed limitations, as Ransom does not disclose wherein said operational status of the wireless communication device comprises an indication of N messages most frequently received at said device, where N is integer.

As to point C, applicant's arguments are not persuasive, as in the context of wherein said operational status of the wireless communication device comprises an indication of N messages most frequently received at said device, where N is integer. The examiner respectfully disagrees with applicant assertions. Reference A discloses N the number of data being sent by the IEDS to the electric power distribution system "many of the messages" which are computed values such as cost, revenue, consumption. The operational statuses are the minimized or maximized measured. (Paragraph [0065] In the preferred embodiment, the data collection component 250 enables an IED to collect and collate data from either a single or multiple sources via the

network 110. The data collected by the component is stored and can be retrieved by other components of the power management application components 290, or other components implemented on other IED's 102-109 located on the network 110. In the preferred embodiment the Automated Meter Reading component 253 is utilized to allow either the consumers 132, 133 or providers 130, 131 to generate power management reports from the IED data. In the preferred embodiment the electrical power generation management component 260 analyzes data received from IED's 102-109 to either minimize or maximize measured or computed values such as revenue, cost, consumption or usage by use of handling and manipulating power systems and load routing. IED inventory, maintenance and fraud detection component 261, 262, 263 receive or request communications from the IED's 102-109 allowing the power management application to inventory the installed base of IED's 102-109, including establishing or confirming their geographic installation location, or check the maintenance history of all connected IED's 102-109 These power management applications aid in confirming outage locations or authenticating communications to or from an IED 102-109 to prevent fraud and minimize errors. In one embodiment, the IED inventory component 261 utilizes cellular triangulation technologies, or caller ID based geographic locator technologies to determine and verify IED inventories. In the preferred embodiment the fraud detection component 263 further detects device tampering. In the preferred embodiment the power quality monitoring component 264 monitors and processes electric parameters, such as current, voltage and energy which include volts, amps, Watts, phase relationships between waveforms, kWh, kvAr, power factor, and frequency, etc. The power quality monitoring component 264 reports alarms, alerts, warnings and general power quality status, based on the monitored parameters, directly to the appropriate user, such as customers

132, 133 or utilities 130, 131.) Examiner gave the broadest interpretation to the claim language. Applicants arguments to the claim failed to overcome the teaching of Ransom.

D. Applicant argues the rejection under 35 U.S.C. 102(b) under Ransom for claims 8 and 20 as Ransom does not disclose the claimed limitations, as Ransom does not disclose wherein said operational status of the wireless communication device comprises an indication of N messages most frequently received at said device, where N is integer.

As to point D, applicant's arguments are not persuasive, as in context of wherein said operational status of the wireless communication device comprises an indication of available memory at said wireless communication device. . The examiner respectfully disagrees with applicant assertions. Reference A discloses The IED 1002 64 MB memory and 6 GB hard disk with a Pentium .TM. (Paragraph [0097] Referring to FIG. 11, there is shown an exemplary screen display of a Microsoft Excel worksheet which is coupled with the IED 1002 as described above. In this example, the IED 1002 is a model 8500 meter, manufactured by Power Measurement Limited, in Victoria, British Columbia, Canada. The IED 1002 is coupled via a TCP/IP based network with a personal computer having at least 64 MB memory and 6 GB hard disk with a Pentium.TM. III or equivalent processor or better, executing the Microsoft Windows 98.TM. operating system and Microsoft Excel 2000. The computer further includes Microsoft Internet Explorer.TM. 5.0 which

includes an XML parser that receives and parses the XML data fro the meter and delivers it to the Excel worksheet. The worksheet displays real time data received directly from the IED 1002 in an XML format. As the IED 1002 detects and measures fluctuations in the delivered electrical power, it transmits updated information, via XML, to the worksheet which, in turn, updates the displayed data in real time. Note that all of the features of the Microsoft Excel program are available to manipulate and analyze the received real time data, including the ability to specify mathematical formulas and complex equations which act on the data. Further, display templates and charting/graphing functions can be implemented to provide meaningful visual analysis of the data as it is received. Further, the real time data can be logged for historical analysis. In one embodiment, the activation of a new IED 1002 on the network is detected by the worksheet which cause automatic generation of a new worksheet to receive and display data from the new device.) Examiner gave the broadest interpretation to the claim language. Applicants arguments to the claim failed to overcome the teaching of Ransom.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashley d. Turner whose telephone number is 571-270-1603. The examiner can normally be reached on Monday thru Friday 7:30a.m. - 5:00p.m. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached at 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-270-2603. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Patent Examiner:

Ashley Turner

Date:_____

Supervisory Patent Examiner

Nathan Flynn

Date:_____

/Nathan J. Flynn/

Supervisory Patent Examiner, Art Unit 2454